IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Gordon GOOD	§	Confirmation No.:	4076
Serial No.:	09/852,244	§	Group Art Unit:	2437
Filed:	May 10, 2001	§	Examiner:	Paul E. Callahan
For:	Security Policy Management For Network Devices	§	Docket No.:	200704491-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: December 8, 2009

Sir:

Appellant hereby submits this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on October 8, 2009.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment to HPDC was recorded on May 7, 2008, at Reel/Frame 0209090707.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-13.
Claim cancellations:	14, 15, 18, 19, 23, and 32.
Added claims:	14-42.
Presently pending claims:	1-13, 16-17, 20-22, 24-31, and 33-42.
Presently allowed claims:	None.
Presently appealed claims:	1-13, 16-17, 20-22, 24-31, and 33-42.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the final Office action dated July 8, 2009.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable. The specification references are made to the application as filed by Appellant. Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

To support an entity's website operations, a website requires an infrastructure that stores the information provided by that site, responds to user requests for the information, and conducts other types of transactions appropriate to the site.[1] While an entity may create and support its own "website," some entities may desire to have their websites supported by an organization that specializes in such a service, such as a managed service provider.[2] In such a situation, employees of the various entities may require access to the servers and other devices that support their respective websites, for example to update content, perform routine maintenance, etc.[3] At the same time, personnel at the support organization also require access to these devices, to upgrade, reconfigure or retire components of the infrastructure.[4] When a single organization is responsible for supporting the data of multiple entities, and different groups of people require access to that data, a problem

[1] P. 1, lines 21-24.

[2] P. 2, lines 11-13.

[3] P. 2, lines 13-16.

[4] P. 2, lines 16-18.

may arise in supporting the individual needs of each of the various entities.[5] For example, each of the respective entities can have specific policies or procedures with regard to their respective information.[6] For example, security polices may be established which define who has permission to access what information.[7] Such a security policy can establish that a particular individual has the authority to access all devices associated with a particular entity, whereas other individuals such as developers may only be authorized to access a subset of the devices associated with the entity.[8]

A common solution involves manually configuring each device.[9] For example, each device may be configured with access lists or user-password pairs that identify who has access to the device.[10] This solution, while providing some data security, has its limitations.[11] For example, when the system requires updating, it can be difficult to find all of the instances of, for example, the user-password pairs, leaving the system vulnerable to unauthorized access.[12] Furthermore, the infrastructure required to support large websites may include numerous computing devices, such as web servers, database servers, and application servers, requiring significant maintenance effort.[13]

Appellant has devised techniques for implementing security policy by means of machine-readable descriptions (*i.e.*, account templates).[14] The templates represent policies applicable to all of the computing devices within a

---

[5] P. 2, lines 18-21.

[6] P. 2, lines 21-22.

[7] P. 2, lines 22-24.

[8] P. 2, lines 24-27.

[9] P. 2, lines 28-29.

[10] P. 2, line 29 to P. 3, line 1.

[11] P. 3, lines 1-2.

[12] P. 3, lines 2-5.

[13] P. 3, lines 5-8.

[14] P. 3, lines 15-17.

network, polices applicable to only a subset of the computing devices, and/or polices applicable to an individual computing device within the network.[15]

The invention of claim 1 is directed to a method for automatically provisioning a plurality of computing devices in accordance with established policies. A plurality of templates reflecting the policies is created.[16] At least one template is expanded at a central location to create a document comprising expanded information.[17] The document comprising the expanded information is sent from the central location to the plurality of computing devices.[18]

The invention of claim 8 is directed to a system for automatically provisioning a plurality of computing devices in accordance with established policies. The system includes a database system 32, a plurality of agents 36, and a communications gateway 38.[19] The database system 32 stores a plurality of templates which reflect the policies.[20] The agents 36 are respectively resident on each of the plurality of computing devices, and communicate with the database system to obtain information with regard to provisioning and maintenance of the respective computing devices.[21] Communication messages are exchanged between the agents 36 and the database system 32 through the communications gateway 38.[22] The communications gateway 38 is configured to: retrieve individual ones of the plurality of templates; expand the retrieved templates to create respective documents containing combined template information and expanded information; and provide the documents containing

---

[15] P. 3, lines 17-19.

[16] Fig. 4a, 402, 204, 406; P. 9, lines 21-27.

[17] Fig. 4a, 408, 410, 412; P. 9, line 28 to P. 10, line 5.

[18] Fig. 4a, 414, 416; P. 10, lines 4-5.

[19] Fig. 3; P. 5, line 26 to P. 6, line 4; P. 6, lines 21-23.

[20] P. 6, lines 8-9; P. 7, lines 1-4.

[21] P. 5, lines 1-3.

[22] P. 6, lines 23-27.

the combined template information and expanded information to the plurality of agents 36.[23]

The invention of claim 22 is directed to a method of controlling user access to networked computing devices. A plurality of templates that identify user-access policies for respective ones of said devices is stored.[24] At least one of the templates includes a reference to information that is external to the template.[25] A template that pertains to a given one of the devices is retrieved, and a document comprising a listing of users identified in the template and users identified by any externally referenced information is created at a central location 38.[26] The document is sent from the central location 38 to the given one of the devices.[27]

The invention of claim 31 is directed to a method for controlling user access to networked computing devices. A plurality of templates that identify user-access policies for respective ones of the devices is stored.[28] At least one of the templates includes a conditional statement.[29] A template that pertains to a given one of the devices is retrieved, and a document comprising a listing of users identified in the template, and users identified in any conditional statement if said given device meets the condition, is created at a central location 38.[30] The document is sent from the central location 38 to the given one of the devices.[31]

---

[23] P. 6, lines 23-27; P. 10, lines 1-4; P. 10, line 4-5.

[24] P. 7, lines 1-4. P. 6, lines 4-6.

[25] P. 8, lines 8-10.

[26] Fig. 4, 408-414; P. 8, lines 29-33; P. 9, line 28 to P. 10, line 4; P. 6, lines 23-27.

[27] Fig. 4 416; P. 10, lines 4-5.

[28] P. 7, lines 1-4; P. 6, lines 4-6.

[29] P. 8, lines 8-11.

[30] Fig. 4, 408-414; P. 9, line 28 to P. 10, line 4; P. 9, lines 3-20; P. 6, lines 23-27.

[31] Fig. 4 416; P. 10, lines 4-5.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-13, 16, 17, 20-22, 24-31, 33-36, 39, and 41 are anticipated by Rothermel et al. (U.S. Pat. No.6,678,827, hereinafter "Rothermel").

Whether claims 37, 38, 40, and 42 are obvious over Rothermel in view of Teng et al. (U.S. Pat. No. 7,380,008, hereinafter "Teng").

VII. ARGUMENT

A. Rejection of Claims 1-13, 16, 17, 20-22, 24-31, 33-36, 39, and 41 Under 35 U.S.C. § 102(e) as Anticipated by Rothermel

1. Claim 1

Independent claim 1 requires "expanding at least one template at a central location to create a document comprising expanded information; and sending from the central location the document comprising the expanded information to said plurality of computing devices." Template expansion is well known to those skilled in the computer arts to refer to assigning values to variable fields of the template.[32] The PTO interprets claim terms "as they would be understood by one of ordinary skill in the art."[33] The Examiner cites Rothermel, column 4, lines 20-67 as teaching the quoted limitations. Rothermel, column 4, lines 20-67 teaches a "security policy manager device to create a consistent security policy for multiple network security devices ("NSDs") by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information." Thus, Rothermel teaches that the template is distributed to the NSDs; and each copy distributed is then expanded (*i.e.*, the templates are expanded in the NSDs). While claim 1 requires centralized template expansion, Rothermel teaches distributed template expansion.

The Examiner admitted that Rothermel teaches distributed template expansion, and contends that Rothermel also teaches "expansion of a template at a central location with later distribution of the expanded information to a plurality of computing devices."[34] The Examiner cited Rothermel col. 10, line 8 to col. 11, line 17 as allegedly teaching centralized template expansion. The cited portion of Rothermel describes Rothermel Figs. 3A-3E.

---

[32] *See, e.g.*, Free Online Dictionary of Computing defining a template as "a document that contains parameters, identified by some special syntax, that are replaced by actual arguments by the template processing system.

[33] *In re Morris*, 127 F.3d 1048 (Fed. Cir. 1997).

[34] *Final Office Action*, at p. 2 (July 8, 2009).

Rothermel Fig. 3A describes generation of specific network security policies 315, 325, 335 for each of several NSDs from corresponding network profiles 310, 320, 330 and a single template 300.[35] With regard to Fig. 3A, Rothermel simply states that "to generate the specific security policy for each network, the security policy template is combined with the network profile for that network."[36] Rothermel does not teach that the combining is performed at a centralized location and the resulting document sent to the NSF as required by claim 1.

Fig. 3B is a more detailed illustration of security policy 315 of Fig. 3A.[37] Nothing associated with Fig. 3B teaches expansion of the template in a centralized location, and thereafter sending the resulting document to the NSD. Rather, without specifying a location in which expansion occurs, Fig. 3B and associated text merely teach that aliases in the template 300 are replaced with network addresses from the network profile 310.[38]

Figs. 3C-3E teach template creation rather than template expansion.[39] Rothermel security policy templates are defined by selecting aliases for template inclusion.[40] Template creation does not teach a location for template expansion.

In contrast to the lack of template expansion location teaching of Rothermel col. 10, line 8 to col. 11, line 17, Rothermel clearly teaches that a security policy template is sent to an NSD, and then the template is expanded.[41]

With regard to the limitations of claim 1 requiring "sending from the central location the document comprising the expanded information to said plurality of computing devices," the Examiner cited Rothermel, column 4, line 49 through

---

[35] *Rothermel*, col. 10, lines 8-23.

[36] *Rothermel*, col. 10, lines 18-20.

[37] *Rothermel*, col. 10, lines 24-27.

[38] *Rothermel*, col. 10, lines 56-59.

[39] *Rothermel*, col. 10, line 66 to col. 11, line 1.

[40] *Rothermel*, col. 11, lines 1-17.

[41] *E.g., Rothermel*, col. 7, lines 16-26.

column 5, line 13. The cited portion of Rothermel teaches a manager device defining a security policy template, sending a copy of the template to a supervisor device associated with the NSDs, the supervisor device sending a copy of the template to the NSDs, and then configuring the NSD template copies in the NSDs. Thus, Rothermel again teaches distribution of the template and distributed expansion in the NSDs. Rothermel fails to teach "sending the document comprising the expanded information to said plurality of computing devices" as required by claim 1.

For anticipation, "[t]here must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention."[42] For at least the reasons given above, one skilled the computer arts would not find the teachings of Rothermel identical to the invention of claim1.[43] Therefore, Appellant respectfully submits that the Examiner erred in rejecting independent claim 1 and claims 2-7, 20, 21, and 39 depending therefrom.

2. Claim 8

Independent claim 8 requires "a communications gateway through which communication messages are exchanged between said agents and said database system, wherein said communications gateway is configured to: retrieve individual ones of the plurality of templates; expand the retrieved templates to create respective documents containing combined template information and expanded information; and provide the documents containing the combined template information and expanded information to said plurality of agents." The Examiner cited Rothermel, col. 4, lines 49-67 as allegedly teaching these limitations. The teaching of the cited portion of Rothermel is explained above with regard to claim 1. The Examiner alleges that the

---

[42] *Scripps Clinic & Research Foundation v. Genentech*, Inc., 927 F.2d 1565 (Fed. Cir. 1991).

[43] *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989) ("The identical invention must be shown in as complete detail as is contained in the ... claim").

Rothermel "manager device" performs the functions required the gateway,[44] and alternately identifies the "supervisor devices" as the communications gateway.[45] However, as explained with regard to claim 1, the Rothermel template is distributed to the NSDs, and thereafter expanded. Consequently, neither the "device manager" nor the "supervisor device" operate to "expand the retrieved templates to create respective documents containing combined template information and expanded information; and provide the documents containing the combined template information and expanded information to said plurality of agents" as required by claim 8. For at least these reasons, Appellant respectfully submits that the Examiner erred in rejecting independent claim 8 and claims 9-13, 16, 17, and 41 depending therefrom.

3. Claim 22

Independent claim 22 requires "creating a document at a central location comprising a listing of users identified in said template and users identified by any externally referenced information." The Examiner rejected claim 22 on the bases applied to claims 1-14, 16-18, 20, and 21.[46] However, none of the referenced claims requires a "listing of users identified in said template" in addition to users identified by externally referenced information. Rothermel fails to teach users identified in the template.

Furthermore, as explained with regard to claim 1, Rothermel teaches distributed template expansion rather than centralized template expansion. Thus, Rothermel fails to teach "creating a document at a central location comprising a listing of users identified in said template and users identified by any externally [template] referenced information; and sending said document from said central location to the given one of said devices."

For at least these reasons, Appellant respectfully submits that the Examiner erred in rejecting claim 22 and claims 24-30 depending therefrom.

---

[44] *Final Office Action*, at p. 3 (July 8, 2009).

[45] *Final Office Action*, at p. 7 (July 8, 2009).

[46] *Final Office Action*, at p. 8 (July 8, 2009).

4. Claim 31

Independent claim 31 requires "creating a document at a central location comprising a listing of users identified in said template, and users identified in any conditional statement if said given device meets the condition." The Examiner rejected claim 31 on the bases applied to claims 1-14, 16-18, 20, and 21.[47] However, the referenced claims require neither "a listing of user identified in said template" nor "users identified in any conditional statement." Rothermel fails to teach users identified in the template or users identified in a conditional statement of the template.

Furthermore, as explained with regard to claim 1, Rothermel teaches distributed template expansion rather than centralized template expansion. Thus, Rothermel fails to teach "creating a document at a central location comprising a listing of users identified in said template, and users identified in any conditional statement if said given device meets the condition; and sending said document from said central location to the given one of said devices."

For at least these reasons, Appellant respectfully submits that the Examiner erred in rejecting claim 31 and claims 33-36 depending therefrom.

5. Claims 3 and 9

Claims 3 and 9 require the "plurality of templates includes conditional statements that determine whether a template is to be expanded with predetermined information on the basis of the computing device to which the expanded information is being provided." The Examiner cited Rothermel col. 10, lines 25-35, Fig. 3B, and Fig.8 as allegedly teaching these limitations. Fig. 3B and related text at col. 10, lines 25-35 teach security policy creation by application of the alias "Information Services." Rothermel teaches that "[i]n general, a network profile contains an alias definition like alias definition 311 for each alias used in the security policy template."[48] "[F]or each . . . rule in security policy template 300, each occurrence of an alias is replaced with the network

---

[47] *Final Office Action*, at p. 8 (July 8, 2009).

[48] *Rothermel*, col. 10, lines 44-46.

addresses of the network elements defined to be within the alias in the network profile 310."[49] Thus, Rothermel fails to teach that rule 301 includes a conditional statement that determines whether the template is to be expanded, but rather teaches only that the template is expanded based on the network profile 310.

Fig. 8 is a flow diagram of a subroutine 720 that determines whether network packets match one or more security policy filter rules.[50] Thus, Fig. 8 teaches application of security policy rather than conditional template expansion.

For at least these additional reasons, Appellant respectfully submits that the Examiner erred in rejecting claims 3 and 9, and claims 4-6 and 21, and 10-12 and 17 respectively depending from therefrom.

6. Claims 5, 11, 27 and 33

Claims 5 and 11 require "the plurality of templates includes a second category of templates that reflect policies applicable to only a subset of the plurality of computing devices." The Examiner cited Rothermel col. 6, lines 22-32 as allegedly teaching these limitations. The cited portion of Rothermel teaches that different classes of devices are defined, with different security policies for each class.[51] However, the existence of different classes of devices with different levels of trust does not necessarily require a first category of templates applicable to all of the plurality of devices (per claims 4 and 10) and a second category of templates applicable to only a subset of the plurality of devices. For example, a single template sent to an NSD may include rules individually applicable to different device classes. Rothermel, Figs. 3A teaches use of a single template 300 to generate different security policies 315, 325, 335 for different networks. Thus, Rothermel fails to expressly teach and does not require multiple categories of templates as required by claims 5 and 11. For at

[49] *Rothermel*, col. 10, lines 56-59.

[50] *Rothermel*, col. 15, lines 30-33.

[51] *Rothermel*, col. 6, lines 21-23.

least these additional reasons, Appellant respectfully submits that the Examiner erred in rejecting claims 5 and 11.

Claims 27 and 33 includes limitations similar to those of claims 5 and 11. Appellant respectfully submits that the Examiner erred in rejecting claims 27-30 and 33-36 for much the same reason as claims 5 and 11.

7. Claims 6 and 12

Claims 6 and 12 require "the plurality of templates includes another category of templates that reflect policies applicable to only a particular type of the plurality of computing devices." The Examiner cited Rothermel col. 6, lines 22-32 as allegedly teaching these limitations. The cited portion of Rothermel is explained above with regard to claims 5 and 11, and fails to expressly or inherently teach multiple template categories. Appellant respectfully submits that the Examiner erred in rejecting claims 6 and 12 for much the same reasons as claims 5 and 11.

8. Claim 24

Claim 24 requires "said external information comprises a list of users." The Examiner cited Rothermel, col. 11, lines 18-30 as allegedly teaching these limitations. The cited portion of Rothermel teaches including customer contact information in a security policy.[52] Claim 24 recites "a method of controlling user access." The "users" of claim 24 are therefore those whose access is controlled. Rothermel fails to teach that the customer contact is a "user" of the computing device to which the template applies to "control user access," but rather simply a contact person with the customer entity. For at least this additional reason, Appellant respectfully submits that the Examiner erred in rejecting claims 24-25.

9. Claims 28 and 34

Claims 28 and 34 require "a template in said second category inherits policies contained in a template of said first category." Per claim 27 and 33, the first category pertains to all of the devices and the second category pertains to

[52] *Rothermel*, col. 11, lines 24-26.

subset of the devices. The Examiner apparently rejected claim 28-30 and 34-36 on the same grounds as claims 4-6 and 10-12.[53] The Examiner contended that "claims 4-6 and 10-12 are worded such that the security policies are in some cases applicable to all, or to only a subset of set of a plurality of devices, and that this is synonymous to the claim language of claims 28-30 and 34-36 where a template in a second category inherits policies contained in a first category and where such inheritance can be selectively disabled."[54] However, the existence of template categories per claims 4-6 is different from "a template in said second category [i.e. pertaining to a subset] inherit[ing] policies contained in a template of said first category [i.e. pertaining to all]." The existence of categories has nothing to do with inheritance across categories or more specifically across narrowing categories. Neither the portion of Rothermel cited against claims 4-6, nor any other portion of Rothermel, teaches inheritance across template categories. For at least this additional reason, Appellant respectfully submits that the Examiner erred in rejecting claims 28-30 and 34-36.

10. Claims 29 and 35

Claims 29 and 35 require that "inheritance can be selectively disabled." As explained above, the Examiner rejected these claims on the grounds applied to claims 4-6. However, the existence of template categories per claims 4-6 is different from policy inheritance across template categories that "can be selectively disabled." Neither the portion of Rothermel cited against claims 4-6, nor any other portion of Rothermel, teaches selectively disabled inheritance across template categories. For at least this additional reason, Appellant respectfully submits that the Examiner erred in rejecting claims 29 and 35.

---

[53] *Final Office Action*, at p. 4 (July 8, 2009).

[54] *Id.*

B. Rejection of Claims 37, 38, 40, and 42 under 35 U.S.C. § 103 as Obvious over Rothermel in view of Teng

Claim 37, 38, 40, and 42 depend from independent claims 31, 22, 1, and 8 respectively. Teng fails to satisfy the deficiencies of Rothermel explained above with regard to claims 31, 22, 1, and 8. Consequently, no combination of Teng and Rothermel teaches or even suggests the limitations of claims 31, 22, 1, and 8. Appellant respectfully submits that the Examiner erred in rejecting claims 37, 38, 40, and 42 for much same reasons as those given above with regard to claims 31, 22, 1, and 8.

C. Conclusion

For the reasons stated above, Appellant respectfully submits that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/David M. Wilson/

David M. Wilson
PTO Reg. No. 56,790
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANT

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528-9599

VIII. CLAIMS APPENDIX

1. A method for automatically provisioning a plurality of computing devices in accordance with established policies, the method comprising the steps of:

creating a plurality of templates reflecting said policies;

expanding at least one template at a central location to create a document comprising expanded information; and

sending from the central location the document comprising the expanded information to said plurality of computing devices.

2. The method of claim 1, further comprising interpreting the expanded information by agents which are respectively resident on each of said plurality of computing devices.

3. The method of claim 1, wherein the structure of said plurality of templates includes conditional statements that determine whether a template is to be expanded with predetermined information on the basis of the computing device to which the expanded information is being provided.

4. The method of claim 3, wherein the plurality of templates includes a first category of templates that reflect policies applicable to all of the plurality of computing devices.

5. The method of claim 4, wherein the plurality of templates includes a second category of templates that reflect policies applicable to only a subset of the plurality of computing devices.

6. The method of claim 4, wherein the plurality of templates includes another category of templates that reflect policies applicable to only a particular type of the plurality of computing devices.

7. The method of claim 1, wherein said policies are security polices regarding user access to each of the plurality of computing devices.

8. A system for automatically provisioning a plurality of computing devices in accordance with established policies, the system comprising:

a database system which stores a plurality of templates which reflect said polices;

a plurality of agents which are respectively resident on each of said plurality of computing devices, and which communicate with said database system to obtain information with regard to provisioning and maintenance of the respective computing devices; and

a communications gateway through which communication messages are exchanged between said agents and said database system, wherein said communications gateway is configured to:

retrieve individual ones of the plurality of templates;

expand the retrieved templates to create respective documents containing combined template information and expanded information; and

provide the documents containing the combined template information and expanded information to said plurality of agents.

9. The system of claim 8, wherein the structure of said plurality of templates includes conditional statements that determine whether a template is to be expanded with predetermined information on the basis of the computing device to which the expanded information is being provided.

10. The system of claim 9, wherein the plurality of templates includes a first category of templates that reflect policies applicable to all of the plurality of computing devices.

11. The system of claim 10, wherein the plurality of templates includes a second category of templates that reflect policies applicable to a subset of the plurality of computing devices.

12. The system of claim 10, wherein the plurality of templates includes another category of templates that reflect policies applicable to a particular type of the plurality of computing devices.

13. The system of claim 8, wherein said policies are security polices regarding user access to each of the plurality of computing devices.

16. The system of claim 41 wherein said external information comprises a list of users.

17. The system of claim 9 wherein said communications gateway expands a template to include information contained in a conditional statement only if the computing device to which said expanded information is to be provided meets the condition.

20. The method of claim 39, wherein said external information comprises a list of users.

21. The method of claim 3, wherein said expanding step includes the step of including information contained in a conditional statement only if the computing device to which said expanded information is to be provided meets the condition.

22. A method of controlling user access to networked computing devices, comprising the steps of:

storing a plurality of templates that identify user-access policies for respective ones of said devices, at least one of said templates

including a reference to information that is external to the template;

retrieving a template that pertains to a given one of said devices and creating a document at a central location comprising a listing of users identified in said template and users identified by any externally referenced information; and

sending said document from said central location to the given one of said devices.

24. The method of claim 22 wherein said external information comprises a list of users.

25. The method of claim 24 wherein all of the users on said list perform a specified role relative to said computing devices.

26. The method of claim 22 wherein at least one of said templates includes a conditional statement, and the step of creating a document comprises including information from said conditional statement in said document only if said given device meets the condition.

27. The method of claim 22, wherein said plurality of templates are classified into at least two categories, wherein a template in a first category pertains to all

of the computing devices, and a template in a second category pertains to a subset of said computing devices.

28. The method of claim 27, wherein a template in said second category inherits policies contained in a template of said first category.

29. The method of claim 28, wherein said inheritance can be selectively disabled.

30. The method of claim 28, further including a third category of templates that pertain to specific devices and inherit policies from templates in said second category.

31. A method for controlling user access to networked computing devices, comprising the steps of:

storing a plurality of templates that identify user-access policies for respective ones of said devices, at least one of said templates including a conditional statement;

retrieving a template that pertains to a given one of said devices and creating a document at a central location comprising a listing of users identified in said template, and users identified in any conditional statement if said given device meets the condition; and

sending said document from said central location to the given one of said devices.

33. The method of claim 31, wherein said plurality of templates are classified into at least two categories, wherein a template in a first category pertains to all of the computing devices, and a template in a second category pertains to a subset of said computing devices.

34. The method of claim 33, wherein a template in said second category inherits policies contained in a template of said first category.

35. The method of claim 34, wherein said inheritance can be selectively disabled.

36. The method of claim 34, further including a third category of templates that pertain to specific devices and inherit policies from templates in said second category.

37. The method of claim 31, wherein said document is an XML document.

38. The method of claim 22, wherein said document is an XML document.

39. The method of claim 1, wherein at least one template includes a reference to information external to the template, and wherein said expanding step comprises creating the document that includes information contained in the template and said external information.

40. The method of claim 39, wherein said document is an XML document.

41. The system of claim 8, wherein at least one template includes a reference to information external to the template, and wherein said communication gateway expands the template by creating a document that includes information contained in the template and said external information.

42. The system of claim 41 wherein said document is an XML document.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.